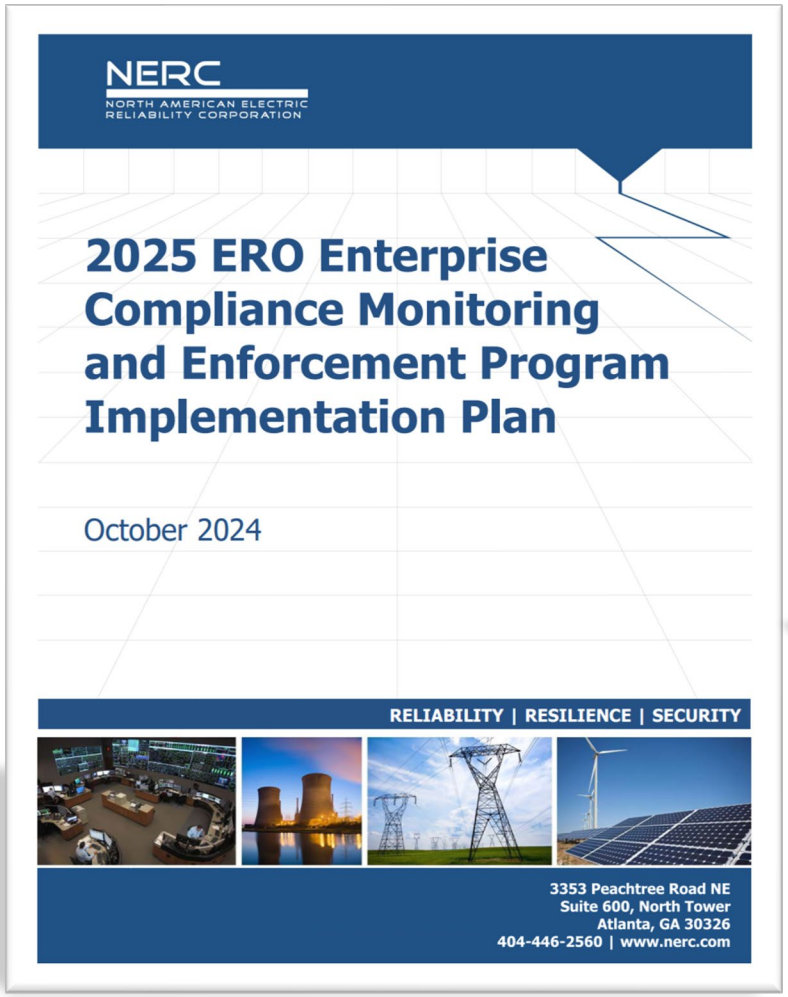
TEXAS RE

CIP-003-8 R2, Section 2

Paul Hopson
CIP Compliance Team Lead

June 6, 2025

2025 ERO CMEP IP: Physical Security



Physical Security

Physical security threats continue to be a top concern in 2025 as threat levels have remained elevated. An area of particular focus should be opportunistic domestic violent extremists. They aim to exploit potential social unrest such as political elections, economic issues, and activistic causes to target infrastructure.[13] More than ever, there are more entities with assets that contain low impact BES Cyber Systems being registered across the ERO. There needs to be a concerted effort around these assets that contain low impact BES Cyber Systems as there has been an upward trend in violations regarding physical security plans, electronic security perimeters, and access management and revocation to name a few.[14] One of the many challenges of executing a physical security program is managing tasks that require repetitive behavior over significant periods of time, as there is increased potential for personnel to lose focus on the performance of an individual act or forget the importance of the act itself. Examples of this behavior that has been observed would be that in multiple instances, an employee who was running late to a shift, without their badge, was able to talk their way through multiple barriers and into a Physical Security Perimeter (PSP).[15] This theme highlights examples of apathy, circumvention, complacency, inattentiveness, and other types of "performance drift" in physical security programs at entities of every size and type.[16]

Risk Element Areas of Focus: Physical Security

CIP-003-8 R2, Section 2: Physical Security

Table 4: Physical Security			
Rationale	**Standard**	**Req**	**Entities for Attention**
Mitigate risks to the reliable operation of the BES as the result of increased Physical Security events related to low impact assets.	CIP-003-8	R2	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner

CIP-003-8 R2, Section 2

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

- **Attachment 1.** Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems
  - Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.
  - Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets
    - **Section 2.** Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

CIP-003-8 R2, Section 2

Control Physical Access

Asset containing a low impact BES Cyber System

Low impact BES Cyber System at the asset

Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any

Examples of Physical Security Controls

BES Asset Level Controls

1. Physical barriers
2. Gates and physical access control
3. On-site security guards
4. Warning signs
5. Lighting and motion sensors
6. Closed-circuit television (CCTV cameras)
7. Intrusion detection system (IDS) (alarm systems)
8. Operational and procedural controls

Low Impact BCS Location Physical Security Controls

1. Doors and locks
2. Physical Access Control System (PACS)
3. Authentication systems
4. Physical intrusion detection systems (IDS)
5. Video management systems (VMS)

Best Practices

Use multiple physical security controls in various combinations to enable and achieve a layered physical security design.

- Multiple controls working together will result in a higher level of protection and minimize physical security risks.

Consider developing and documenting a diagram or schematic of the BES asset layout and locations of Cyber Assets.

- Illustrate on the diagram the locations and brief description of where physical security controls are deployed and their intended purpose. This can provide a quick reference to understand how and where physical security controls have been implemented.

TEXAS RE
Ensuring electric reliability for Texans